

CLAIMS

What is claimed is:

1 1. A method of providing secure access to content comprising:
2 determining a secure medium identification (disk ID) from a secure
3 medium including content;
4 sending a session key and the disk ID to a server;
5 requesting user authentication; and
6 if the user is successfully authenticated, receiving the session key from the
7 server to enable reading of the content on the secure medium.

1 2. The method of claim 1, further comprising:
2 streaming encrypted content to an application.

1 3. The method of claim 2, further comprising;
2 the application using the session key returned by the server to decrypt the
3 encrypted content, and display the content.

1 4. The method of claim 1, wherein the content is stored as encrypted
2 content on the secure medium.

1 5. The method of claim 4, further comprising:
2 receiving a content decryption key from the server, in response to the disk
3 ID and the user authentication.

1 6. The method of claim 5, wherein the content decryption key is
2 determined based on the disk ID.

1 7. The method of claim 6, further comprising:
2 the application using the content decryption key and the session key
3 returned by the server to decrypt the content received from the secure medium;
4 and
5 playing the content.

1 8. The method of claim 1, further comprising a trusted device for
2 accessing secure content:
3 reading the disk ID from the secure medium and generating a one-time
4 session key; and
5 sending an encrypted copy of the disk ID and session key to the server.

1 9. The method of claim 8, wherein the disk ID and session key are
2 encrypted using a symmetric key.

1 10. The method of claim 1, wherein the secure medium is selected from
2 among the following: an optical disc, a flash memory, a hard drive, a magnetic
3 drive, a memory stick, or another type of storage device.

1 11. The method of claim 1, wherein the content is digitally encoded
2 music.

1 12. The method of claim 1, wherein user authentication comprises one
2 or more of the following: a credit card, a debit card, electronic cash, a user-
3 specific ID card.

1 13. The method of claim 1, wherein the user authentication comprises
2 one or more of the following: a password, a user identification, a biometric
3 identification.

1 14. The method of claim 1, wherein authenticating the user comprises:
2 determining if the disk ID is already associated with a user; and
3 if the disk ID is not yet associated with the user, associating the user
4 authentication data with the disk ID.

1 15. The method of claim 15, further comprising:
2 if the disk ID is associated with a user, determining that the current user
3 authentication matches the user associated with the disk ID, to authenticate the
4 user.

1 16. The method of claim 15, further comprising:
2 if the user authentication does not match the user associated with the disk
3 ID, refusing to return the session key, thereby preventing display of the content.

1 17. An apparatus comprising a secure device for accessing secure
2 content coupled to a client system comprising:
3 a reader to read an identification (ID) and content from a secure medium;
4 an encryption logic to send the ID encrypted to a server;
5 an authentication logic to receive authentication from the server
6 indicating approval to read the content of the secure medium;
7 the reader further to read the content; and

8 the encryption logic further to encrypt the content prior to sending the
9 content to an application.

1 18. The apparatus of claim 17, wherein the encryption logic uses a
2 symmetric key to encrypt the ID.

1 19. The apparatus of claim 17, further comprising:
2 a session key generation logic to generate a one-time session key, the
3 session key send with the ID to the server.

1 20. The apparatus of claim 17, further comprising an application on the
2 client system comprising:
3 a user authentication interface to request a user authentication in response
4 to a server request, and to send the data received from a user to the server;
5 a key logic to receive a decryption key from the server, if the user is
6 successfully authenticated; and
7 a streaming decryption logic to receive data from the secure device and
8 decrypt the data using the key received from the server, and play the data.

1 21. The apparatus of claim 20, wherein the decryption key is a session
2 key and a content decryption key.

1 22. The apparatus of claim 17, further comprising a secure server
2 coupled to the client system via a network, the secure server comprising:
3 a network interface to receive the ID and a session key from the secure
4 device;

5 a user validation logic to request a user validation from the client system
6 and determine whether the user has permission to access the secure medium
7 identified by the ID; and
8 an encryption logic to return the session key and a content decryption key
9 if the user has permission to access the secure medium.

1 23. The apparatus of claim 22, further comprising:
2 the encryption logic further to decrypt data received from the secure
3 device using a symmetric key.

1 24. The apparatus of claim 22, further comprising:
2 an ID lookup to determine the content decryption key based on the ID.

1 25. A client system to securely access digital content on a secure
2 medium, the client system comprising:
3 a secure device comprising:
4 a reader to read an ID and content from the secure medium;
5 an authentication logic to receive authentication from the server
6 indicating approval to read the content of the secure medium;
7 and
8 an encryption logic further to encrypt the content prior to sending
9 the content to an application;
10 an application comprising:
11 a user authentication interface to request a user authentication in
12 response to a server request, and to send the data received
13 from a user to the server;

14 a key logic to receive a decryption key from the server, if the user is
15 successfully authenticated; and
16 a streaming decryption logic to receive data from the secure device
17 and decrypt the data using the key received from the server,
18 and play the data.

003551.P015